Department of Homeland Security Daily Open Source Infrastructure Report for 09 February 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- KTUL TV reports a massive Hexane chemical fire in Tulsa, Oklahoma, destroyed three businesses and forced the evacuation of a quarter−mile area. (See item 5)
- Computerworld reports a "human error" at Blue Cross and Blue Shield of North Carolina allowed the Social Security numbers of more than 600 members to be printed on the mailing labels of envelopes sent to them with information about an insurance plan. (See item 12)
- Central Valley Business Times reports the California state veterinarian says farmers, ranchers, and others involved in the food industry should develop security plans for their own businesses, and that non−terrorist threats must also be dealt with. (See item 20)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *February 08, Triangle Business Journal (NC)* — **Nuke regulators approve $9 billion Duke purchase.** The U.S. Nuclear Regulatory Commission has approved Duke Energy Corp.'s planned $9 billion acquisition of Cinergy Corp. The companies' shareholders are slated to vote on the deal March 10. Meanwhile, regulatory approvals are pending in North Carolina and Indiana. Last week, thousands of employees of Duke and Cinergy received voluntary severance

offers as part of a goal of eliminating 1,500 positions, or about five percent of the companies' 30,000−employee staff. Labor cost savings are a key factor in the economics of merger, which was announced in May. Labor−force cuts are expected to comprise about 40 percent of the savings. The severance offers are aimed mostly at white−collar employees; most nuclear operations and maintenance workers will not be offered packages, Duke spokesperson Randy Wheeless said. Cinergy has 7,286 employees, down by 154, or about two percent, from last May. Duke Energy's electric utility, Duke Power Co., serves the Carolinas. Cinergy provides electricity service in Indiana, Ohio, and Kentucky. The merger, scheduled to close in April, will create one of the nation's biggest electric utilities.
Source: http://www.bizjournals.com/triangle/stories/2006/02/06/daily 20.html?from_rss=1

2. *February 07, Canadian Press* — **Russia pushes nuclear development plan without military implications.** As global anxieties grow over Iran's alleged atomic bomb program, Russia, with U.S. backing, has floated a plan to help energy−starved countries obtain access to nuclear power while restricting the flow of weapons−grade uranium to those who might harbor military ambitions. The scheme, announced by President Vladimir Putin at a news conference last week, would extend to all countries a similar deal to the one Russia has offered to defuse Iran's nuclear crisis. Under its terms, the vulnerable stages of the nuclear fuel cycle −− uranium enrichment and radioactive waste disposal −− would be confined to a few specialized centers in Russia and the U.S. That would plug a loophole in the current nuclear non−proliferation regime, which allows countries to enrich uranium as long as it's for "peaceful " purposes. That's the nub of the world's current worries over Iran's intentions. At a meeting last week of the International Atomic Energy Agency, Russia voted to report Iran's suspected nuclear misconduct to the United Nations Security Council, but any action will be postponed for a month. Negotiations over Moscow's offer to transfer Iran's uranium enrichment to Russian facilities are set to resume on February 16.
Source: http://news.yahoo.com/s/cpress/20060207/ca_pr_on_wo/russia_i ran_nuclear_1

3. *February 07, Reuters* — **Petroecuador suspends oil exports amid protest.** Ecuador's state oil company Petroecuador suspended oil exports on Tuesday, February 7 after hundreds of protesters stormed a pumping station and demanded the government quit trade talks with the United States. Citing the protests, Petroecuador declared force majeure, freeing it from its contractual obligations. The company shut down its 380,000 barrels−per−day Sote Trans−Ecuadorean pipeline after hundreds of protesters burst into the station at Baeza demanding the government suspend trade talks with the United States and expel Occidental Petroleum over a disputed contract. The pipeline moves all of Petroecuador's production. The fight with Occidental stems from the company's disputed transfer of an oil block to a Canadian oil company without notifying the Ecuadorean government. Ecuadorean officials accuse Occidental of transferring 40 percent of an oil field to Canada's EnCana Corp. without government authorization and in violation of a contract with Petroecuador. "We haven't done anything that we aren't allowed to do under the law and our contract," said Occidental's legal vice president in Ecuador, David Almaguer. Occidental produces around 100,000 bpd of oil or around 20 percent of Ecuador's production. The U.S. Energy Information Administration reports that in 2004, Ecuador was the 13th top supplier of U.S. crude oil and petroleum.
Source: http://today.reuters.com/business/newsarticle.aspx?type=tnBu sinessNews&storyID=nN07254155&imageid=&cap=

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *February 08, Houston Chronicle (TX)* — **Explosions and smoke close parts of busy roads in Texas.** Tuesday afternoon, February 7, a fire and subsequent small explosions occurred at the Akzo Nobel Chemicals plant in Deer Park, TX, injuring one employee. The fire caused officials to close part of busy Texas−225 and Battleground Road in east Harris County during the afternoon traffic rush. Mildred Hughes, process and quality control manager of the plant, said the fire broke out about 3:25 p.m. CST in a warehouse in the handling area of the plant that produces aluminum alkyls. The product is used to make plastics. The fire did not prompt any evacuations or alarms for residents to stay indoors. The Harris County Sheriff's Department issued a brief shelter in place advisory for the area north of Texas−225.
Source: http://www.chron.com/disp/story.mpl/metropolitan/3643648.htm l

5. *February 07, KTUL TV (OK)* — **Chemicals from business fire cause for concern in Oklahoma.** Firefighters remained on the scene of a massive fire in Tulsa, OK, that destroyed three businesses well into the evening Tuesday, February 7. The fire also forced the evacuation of a quarter−mile area including the Woodland Broken Arrow Animal Hospital. It erupted just before 2 p.m. CST on Tuesday afternoon near 71st Street and 145th East Avenue in Broken Arrow. At the peak of the fire, smoke was billowing high into the air and could be seen for miles. Because there were so many chemicals involved, firefighters took every precaution for their own safety and evacuated the area for the protection of others. Investigators have identified the primary chemical involved as Hexane, which is most dangerous in its liquid form and is often mixed with solvents for cleaning purposes.
Source: http://www2.ktul.com/news/stories/0206/300969.html

[Return to top]

Defense Industrial Base Sector

6. *February 08, Defense News* — **U.S. Navy fleet plan sent to Congress.** The long−awaited 30−year shipbuilding plan of Adm. Mike Mullen, U.S. Navy chief of operations, is now official. The strategy to build a 313−ship fleet was sent to Congress Tuesday, February 7, after having been endorsed by Defense Secretary Donald Rumsfeld. The official plan commits the Navy to a force of 11 aircraft carriers −− dropping to 10 in fiscal 2013 and rising to 12 ships beginning in 2019. The submarine force hovers around a median of 48 boats, from a high of 55 subs in 2018 to a low of 40 in 2028, before rising to 51 boats in 2036. The plan also provides for 55 Littoral Combat Ships, a figure planned to be attained in 2018. “The goal is to have a plan which is stable and industry can build to,” he said. Having spent much of his seven months in office focusing on shipbuilding and the Quadrennial Defense Review (QDR), Mullen said he would begin looking at the aviation side of the Navy’s planning efforts. “That’s what we’ll do for the ’08 budget,” he said.
Source: http://www.defensenews.com/story.php?F=1519940&C=america

7.

February 07, GovExec — **Pentagon's business transformation effort moves forward.** Details are emerging on how the Pentagon's newly formed agency for renovating business processes is structured and what its budget could look like in fiscal 2007. The Defense Department's Business Transformation Agency (BTA) consists of seven divisions, according to a memorandum issued Friday, February 3, and published on the agency's recently launched Website. The recently established agency moves dozens of the Pentagon's most extensive business modernization programs under a single roof and centralizes oversight of 18 department−wide programs. In his fiscal 2007 budget request, unveiled Monday, February 6, President Bush proposed $179 million for the business agency. If Congress enacts his request, BTA would get an additional $16.3 million for procurement programs and $140 million for research, development, test and evaluation programs. Goals for Business Transformation Agency described in the budget proposal include the development of department−wide business processes aligned with those in the private sector. The agency reports to the Defense Business Systems Management Committee and is under the authority of Defense Undersecretary for Acquisition, Technology and Logistics Kenneth Krieg, according to the memo and budget documents.
Defense Business Transformation Website: http://www.dod.mil/dbt/
Business Transformation Agency: http://www.dod.mil/bta/
Source: http://www.govexec.com/story_page.cfm?articleid=33347&dcn=to daysnews

[Return to top]

Banking and Finance Sector

8. *February 07, Yahoo! (Asia)* — **Man rearrested in Japan's first phishing fraud case.** Police have served a warrant on a 25−year−old man who was previously arrested on suspicion of phishing fraud, in which he allegedly stole and used personal information from users of Yahoo Japan's Internet auction service, the Tokyo Metropolitan Police Department said Tuesday, February 7. The Tokyo police allege that Sunao Koizumi, using stolen user IDs and passwords, won about 300 bids for a total of about 5.5 million yen worth of book vouchers and travel coupons on Internet auctions and resold the products. This was Japan's first arrest over an alleged fraud case conducted through phishing, a scheme to lure Internet users to a bogus Website that uses the organization's logo to trick users into providing private information. He was quoted of telling police investigators, "I came up with this method myself. I resold the defrauded vouchers to pay my living expenses." Koizumi allegedly obtained the IDs and passwords of about 500 Yahoo auction users between last March and this January. He was arrested Tuesday, January 17 for trespassing when he showed up at an apartment building where he asked for the merchandise to be delivered.
Source: http://asia.news.yahoo.com/060207/kyodo/d8fk4i588.html

9. *February 07, Olympian (WA)* — **Scammers target Providence clients.** Customers of Providence Home Services whose personal information was stolen in a security breach at the company, are now at the whim of scammers who are posing as Providence officials. The scammers have called some people asking for Social Security and bank account numbers. The calls have been reported to Providence and to the Oregon Attorney General’s Office. Providence spokesperson Gary Walker couldn’t say how many calls were reported but said it’s “a pattern.” The calls are a response to the December 31 theft of computer disks containing

patient information on 365,000 Providence Home Services patients in Oregon and Washington. Scammers are pretending to call from Providence saying they need to get personal information to verify the stolen information. Providence officials have sent letters to patients affected by the theft, but have not called any of them. The scammers do not appear to have access to the Providence patient database, but are simply cold−calling people, Walker said. “The vast majority of people who’ve told us they’ve received calls aren’t even Providence patients,” he said. No identity thefts have been reported as a result of the Providence security breach, according to Kristin Alexander, a spokesperson at the Washington attorney general's office.
Source: http://www.theolympian.com/apps/pbcs.dll/article?AID=/200602 07/NEWS/60207004

10. *February 07, Guardian (UK)* — **Sleeper bugs used to steal millions in France.** Russian thieves have stolen millions from personal bank accounts in France. French authorities claim the thieves used so called “sleeper bugs” which can take control of and empty a bank account in seconds. Police say the virus is embedded in e−mails or Websites and remains dormant until the user contacts their bank online. Then the bug becomes active and records passwords and bank codes which are forwarded to the thieves. They use the information to check the victim's account before transferring funds to the accounts of third parties, known as mules, who may have agreed to allow money to pass through their accounts in return for a commission. This may be set up through fictitious companies, including one American firm named World Transfer, although the mules could be unaware that their computers are being used for theft. A dozen Russian thieves between the ages of 20 and 30, and several Ukrainians were arrested in Moscow and St. Petersburg. The authorities were alerted in November 2004, when a bank customer noticed a large sum missing from his account, and reports from all over France followed. Nicolas Woirhaye, a security expert, said the authorities were alerted to scams every three weeks.
Source: http://www.guardian.co.uk/france/story/0,,1703777,00.html

11. *February 07, Websense* — **Day Air Credit Union targeted by phishing attack.** Websense Security Labs has received reports of a new phishing attack that targets customers of Day Air Credit Union. Users receive a spoofed email message, which claims there have been multiple attempts to log on to their account from a foreign IP address. Users are directed to verify their identity by logging on to their account. The message provides a link to a phishing Website that requests account number and password. The phishing site is hosted in Germany and was up at the time of this alert. The e−mail reads: "Dear DAYAIR Credit Union Customer, We recently noticed one or more attempts to log in to your online account from a foreign IP address. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you did not initiate the log ins, please visit dayair.org as soon as possible to verify your identity: Verify your identity is a security measure that will ensure that you are the only person with access to the account. Thanks for your patience as we work together to protect your account. Sincerely, President/CEO, Bill Burke."
Phishing site screenshot: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =420
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =420

12. *February 07, Computerworld* — **Human error exposes patients' Social Security numbers in North Carolina.** A "human error" at Blue Cross and Blue Shield of North Carolina allowed the Social Security numbers of more than 600 members to be printed on the mailing labels of envelopes sent to them with information about a new insurance plan. The mistake affected

patients who had applied for a new health savings account insurance plan, said Gayle Tuttle, a spokesperson for the insurer. “The mailing label on a welcome letter that we sent out to 629 people enrolled in one of our individual insurance plans contained an 11−digit tracking number, nine of which were the members’ Social Security numbers,” Tuttle said. As part of a broader bid to enhance privacy, Blue Cross has been using a new subscriber number instead of Social Security numbers to identify patients, Tuttle said. Even so, there is still a “linking” that goes on internally between the subscriber IDs and Social Security numbers that may have contributed to the error. The problem was discovered on Monday, January 30, and letters were sent to the affected individuals on Wednesday, February 1 informing them of the breach. Blue Cross is now looking at its internal procedures to see how such mistakes can be avoided in future.
Source: http://www.computerworld.com/printthis/2006/0,4814,108444,00 .html

13. *February 06, IDG News Service* — **Honeywell blames former employee in data leak.** Honeywell International Inc. says a former employee has disclosed sensitive information relating to 19,000 of the company's U.S. employees. Honeywell discovered the information being published on the Web on Friday, January 20 and immediately had the Website in question pulled down, said company spokesperson Robert Ferris. In court filings, the company accused former employee Howard Nugent of Arizona of accessing the information on a Honeywell computer and then causing "the transmission of that information." Nugent has since been ordered not to disclose any information about Honeywell, including "information about Honeywell's employees (payroll data, Social Security numbers, personal information, etc.)," according to a January 31 order signed by Judge Neil Wake of the U.S. District Court for the District of Arizona. The precise method Nugent is alleged to have used to gain access to the information, and why he may have disclosed it, is not clear. In the court filings, Honeywell claimed that Nugent "intentionally exceeded authorized access to a Honeywell computer," but the integrity of Honeywell's computer systems was not compromised, Ferris said. "Nobody hacked into systems," he said, without disclosing further details on the data breach. The company is working with federal and local authorities on the case.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,108434,00.html?from=story_package

[Return to top]

Transportation and Border Security Sector

14. *February 08, CNN* — **Fire forces UPS plane to make emergency landing.** A UPS cargo plane made an emergency landing at Philadelphia International Airport early Wednesday, February 8, after a fire broke out on board. Flames were seen coming from the cargo area of the DC−8 when it landed. UPS Flight 1307 landed at 12:22 a.m. EST "after reporting a lower cargo and main deck smoke situation," the company said in a written statement. It took emergency responders more than four hours to douse the fire, said Mark Giuffre, a spokesperson for UPS. The airport, which is usually open 24 hours per day, was shut down after the plane landed, but was reopened at 6 a.m., using only three of its four runways, Giuffre said. The plane's three crewmembers were taken to the University of Pennsylvania Hospital. Giuffre added that the National Transportation Safety Board would investigate. With a fleet of 269 jet aircraft and 305 chartered aircraft, UPS is the world's ninth−largest airline. It has never had a crash, Giuffre said.

Source: http://www.cnn.com/2006/US/02/08/ups.plane.fire/index.html

15. *February 08, Virginian−Pilot (VA)* — **Coast Guard's budget request reflects homeland security role.** The Coast Guard's dramatic evolution from a quiet maritime police force to a mainstay of homeland security is reflected in its budget request to Congress. The proposed $8.4 billion spending plan for fiscal year 2007 would broaden the role of the Coast Guard and update its aging fleet. The budget −− the largest ever sought by the service −− seeks $934.4 million to continue replacing an obsolete fleet of cutters and aircraft, and would include an unmanned aerial vehicle. The budget asks for $62.4 million to create the National Capital Region air defense operation in Washington, DC. Its mission would include the interception of potential threats in Washington air space and would be run by the 5th District, headquartered in Portsmouth, VA. Moving further into counterterrorism, the Coast Guard wants $4.7 million to provide a third 60−member Maritime Security Response Team in Chesapeake, VA, allowing it to operate around−the−clock. Coast Guard officials said the budget request reflects the missions required by the Department of Homeland Security and the need to respond to natural disasters, such as hurricanes. The Coast Guard's Deepwater Project is designed to replace or modernize its 93 cutters and 190 aircraft over an undetermined number of years.
Source: http://home.hamptonroads.com/stories/story.cfm?story=99238&r an=17113

16. *February 08, Star−Telegram (TX)* — **American to offer copter service to NYC airport.** American Airlines has an easy, if expensive, solution for New York City travelers who want to bypass airport traffic: soar over the cars on a helicopter that lands at the airline's terminal. The service, which American is offering through an agreement with US Helicopter, is the Fort Worth−based airline's latest effort to hold onto its premium business customers, who have been targeted by rival United Airlines. "This is really aimed at our high−end customers who are among the largest corporations in New York," American spokesperson Ned Raynolds said. The helicopter flights will be offered starting March 13 between John F. Kennedy International Airport and a Wall Street heliport and will take about eight minutes. They will initially cost $139 each way. A taxi ride between the airport and Manhattan takes 45 minutes or longer, depending on traffic, and typically costs about $30. Travelers who take the helicopter to the airport will save additional time by going through a security checkpoint and checking their bags at the heliport, bypassing lines at the airport. The deal will allow American to provide a service that competitors can't match, at least for now. No other company provides helicopter service at New York's airports.
Source: http://www.dfw.com/mld/dfw/business/13819673.htm

17. *February 08, USA TODAY* — **Radar system spots debris on runway.** The radar system, expected to be installed in early April at Vancouver, Canada's second−busiest airport, continuously monitors for debris. Now, airports rely on periodic visual inspections. U.S. and Canadian airports are required to inspect daily for debris; some do it three or four times each day. The radar will not eliminate nightly visual checks of runway lighting and periodic checks of rubber build−up from aircraft tires. The Federal Aviation Administration finished a 10−day test of the system last January and concluded that the system "was not mature enough" to recommend its use, says agency spokesperson Diane Spitaliere. Since then, the radar system's manufacturer has been working to improve it. Debris on runways became a major safety issue when the French government blamed a metal strip from a Continental Airlines jet for causing a Concorde jet to crash in July 2000, while taking off from Paris. Runway debris is an everyday

concern that annually costs the airline industry an estimated $2.5 billion in aircraft repairs, flight delays and airport maintenance, says Richard Bell, president of non−profit National Aerospace Foreign Object Debris Prevention. Debris commonly found on runways includes bolts and other aircraft parts, dead animals, paper and other litter.
Source: http://www.usatoday.com/travel/news/2006−02−07−runway−radar_x.htm

18. *February 08, San Bernardino County Sun (CA)* — **Border guards seek military's help.** The U.S. military should be called out to protect the border against military−style incursions from Mexico, the head of the Border Patrol union told a congressional homeland security committee on Tuesday, February 7. T.J. Bonner, president of the National Border Patrol Council, which represents 10,500 agents, recommended active or reserve military units be put "on standby" at strategic locations along the border. "If the Mexican military is coming into the United States, our law−enforcement agents do not have the training to deal with that," Bonner told the House Homeland Security subcommittee on Investigations. The proposal was one of several that Bonner and Texas law−enforcement agents laid out as Congress launched its first investigation into Mexican incursions. The hearing, which will be followed by one in the Senate next month, comes in the wake of a high−profile Texas incident in which sheriff's deputies said they confronted drug runners who were wearing Mexican military uniforms, driving a military−issue Humvee and using military tactics. The Mexican Embassy maintains the suspected smugglers, who were not arrested, were members of a drug cartel posing as soldiers, not members of the Mexican military. But Texas officials testifying Tuesday said they think the suspects might be both.
Source: http://sbsun.com/news/ci_3485358

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

19. *February 08, Jackson Hole News (WY)* — **Elk slaughter begins.** Wildlife managers peered down into the largest elk trap ever erected in Wyoming, at the Muddy Creek feed ground, to see how many elk would take the bait. Wildlife managers had been feeding elk inside the trap, 25 miles south of Boulder, for three weeks to accustom the animals to the structure. At a nearby staging area, Wyoming Game and Fish Department managers waited for word of elk entering the corral, measuring 150 feet in diameter. “The elk make the final decision of whether they’re going to cooperate,” said Terry Kreeger, a Game and Fish veterinarian. Such unknowns are one reason Wyoming has launched this pilot program to see whether a test−and−slaughter operation, more commonly used on livestock, could work for wildlife. A state task force recommended launching the five−year program to see whether capturing, testing and slaughtering elk could reduce the prevalence of the disease brucellosis among the 1,911−strong Pinedale elk herd. On Tuesday, February 7, Wyoming shipped 42 elk, which tested positive for brucellosis exposure, to a slaughterhouse in Idaho. Though wildlife managers fell short of their

goal of trapping 80 percent of test−eligible elk, Kreeger said the state has five years to work out kinks in the program.
Brucellosis information: http://168.68.129.70/vs/nahps/brucellosis/
Source: http://www.jacksonholenet.com/news/jackson_hole_news_article.php?ArticleNum=1363

20. *February 08, Central Valley Business Times (CA)* — **Farm security plans urged.** California State Veterinarian Richard Breitmeyer says farmers, ranchers, and others involved in California's food industry should develop security plans for their own businesses. He says regulators need help in developing plans and that a one−size−fits−all approach by regulators would not work. Breitmeyer also cautioned farm leaders that other, non−terrorist, threats must be dealt with, from backyard chicken coops to horses. "We've actually kept a team of about 15 veterinarians and inspectors working in Los Angeles on outreach to backyard poultry owners, not only to look for Exotic Newcastle disease that might reappear but probably more importantly to look for any evidence of avian influenza," Breitmeyer said. Another threat to California agriculture is about to increase as the weather warms, he says. It's the threat of West Nile disease. "We would hope every horse owner by now since this will be our third season addressing West Nile in California have already gotten their horses vaccinated but if not, we really encourage them to contact their veterinarian, get the number of doses needed before mosquito season," Breitmeyer said in an interview with the California Farm Bureau.
Source: http://www.centralvalleybusinesstimes.com/stories/001/?ID=13 04

21. *February 06, Shanghai Daily (China)* — **Disease of 200 cows in Liaoning still unknown.** The pathogeny of more than 200 milch cows in a Liaoning, China, village is still unknown, though farmers have reported the cases to the Ministry of Agriculture twice in the last 12 days, the China Business News said Monday, February 6. Liu Jianhua, a villager of Liangjia Village, reported the first case to the local epidemic prevention station on January 8, after he found some of the milch cows raised by his neighbor excessively salivating and having blisters on their breast skin. On the morning of January 17, Liu found two of his milch cows suffering from the same symptoms. He called the epidemic prevention station again to report it. Half an hour later, the station director came to the Lius, and discovered the cows had fevers of 40.3 degrees Celsius. As of January 19, six cows of Lius were infected and unable to produce milk. Liaoning's veterinary authorities said the outbreak in Liangjia Village was an ordinary epidemic rather than foot−and−mouth disease, according to the China Business News. In Liangjia Village, 26 families raised milch cows. Now 70 percent of the village's 300 milch cows are suffering from the disease.
Source: http://www.shanghaidaily.com/art/2006/02/07/240781/Disease_of_200_cows_in_Liaoning_still_unknown.htm

[Return to top]

Food Sector

22. *February 08, Chicago Sun−Times (IL)* — **Over 100 fall ill after eating at hotel.** More than 100 guests and others who dined at the Drake Hotel, in Chicago, IL, over the weekend have fallen ill, complaining of a stomach−like flu. "Lab results are pending, but clinically and from an epidemiological standpoint, it looks like an outbreak of the norovirus," said Tim Hadac of

the Chicago Public Health Department. Noroviruses are also known as the "Norwalk−like" viruses, and symptoms include vomiting and diarrhea; it can be spread by eating food or drinking contaminated liquids. Sue Wilson said Tuesday, February 7, her Children's Medical Research Foundation Inc. was holding a fund−raiser at the Drake Friday, February 3, and 120 of the 190 in attendance were reportedly sick. At least eight of those who were sick went to hospital emergency rooms, but most were recovering in 24 to 48 hours, health officials said.
Source: http://www.suntimes.com/output/news/cst−nws−drake08.html

23. *February 08, Bloomberg* — **Europe's biotech seed rules ruled illegal by World Trade Organization.** The World Trade Organization (WTO) ruled that the European Union (EU) unfairly blocked imports of genetically engineered crops, U.S. trade officials said, setting a precedent that may force other nations to drop their restrictions. In the first of decision its kind, the WTO sided with the U.S., Canada, and Argentina, saying the EU discriminated against imports of biotech seeds from companies without adequate scientific evidence of their harm, according to people familiar with the case. European governments such as Germany and France, as well as interest groups such as Greenpeace, have sought to curb the use of seeds genetically altered to resist pests, disease, and drought. The WTO ruling sets a precedent for other nations ranging from India to Japan to Russia that have regulations stipulating the labeling and tracing of goods containing biotech ingredients. "One of the main reasons to bring the case was to prevent the loss of other important markets" for U.S. agriculture exports, said Michelle Gorman, director of regulatory relations at the American Farm Bureau Federation. The planting of altered seeds rose to 90 million hectares in 2005 from 1.7 million worldwide since initial commercialization in 1996, industry groups estimate. The U.S. accounts for about 55 percent of that total.
Source: http://www.bloomberg.com/apps/news?pid=10000085&sid=aOhAZsCZvmNU&refer=europe

24. *February 08, Food Navigator* — **System uses Internet and satellites to track food.** A prototype European Union (EU) funded project uses the Internet and satellites to trace the geographic origin of food throughout the supply chain. GeoTraceAgri will provide food processors with precise tracking information about food products, the project's researchers said Tuesday, February 7, in marking the completion of the prototype. From January 1, 2006, new EU food laws introduced mandatory traceability requirements throughout the bloc. Processors must track ingredients from their immediate suppliers and the products to their retail or distribution points. The system will provide information accessible in real−time. The system will cover all stages of production from "farm to fork", including storage, processing, and distribution, according to IST Results, the reporting section of an EU−funded research network. The European Commission has also approved a follow−up project, GTIS CAP (GeoTraceability Integrated System for the Common Agricultural Policy). The aim of the offshoot project will be to design and create an integrated information system serving both regulatory bodies and producers of vegetable food and feed products.
Source: http://www.foodnavigator−usa.com/news/ng.asp?n=65681−geotraceagri−cap−traceability

25. *February 05, Dallas Morning News (TX)* — **Study supports corn toxin as culprit in birth defects.** For more than a decade, scientists have been unable to explain why, starting in 1990, an alarming number of border infants were born with neural tube defects. In Cameron, TX,

alone, six babies with missing or rudimentary brains were born in six weeks. An investigation found a high rate of neural tube defects among almost all border counties. By early 1992, the epidemic had subsided as mysteriously as it appeared. Texas health officials began to suspect a naturally occurring danger: fumonisin, a toxin from mold that can appear on corn crops. Just before the appearance of neural tube defects along the border, agricultural experts had noted high concentrations of fumonisin on that year's corn harvest, and Texas horses were experiencing an outbreak of a fatal brain disease caused by the toxin. The study's major finding: Women who ate 300 to 400 tortillas per month during their first trimester had more than twice the risk of giving birth to a baby with a neural tube defect than women who ate less than 100 tortillas. Blood samples taken from women also indicated that the higher the level of fumonisin, the greater the risk of neural tube defects.
Source: http://www.dallasnews.com/sharedcontent/dws/news/healthscience/stories/DN−corntoxin_05nat.ART.State.Edition1.3e9944f.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

26. *February 08, Associated Press* — **Bird flu found in Africa.** The H5N1 bird flu virus has been detected on a large commercial chicken farm in Nigeria −− the first reported outbreak in Africa, the World Organization for Animal Health (OIE) said Wednesday, February 8. The outbreak appears to be restricted to birds, and no human infections have been reported, the OIE said. Nigeria said the outbreak was on a farm in Jaji, a village in the northern state of Kaduna. Agriculture Minister Adamu Bello told reporters that the H5N1 strain of the virus was detected in samples taken January 16 from birds on the farm. Experts have long been concerned about Africa's ability to deal with a bird flu outbreak. Alex Thiermann, of the OIE, noted that some African countries have "very weak" veterinary systems. Thiermann said all 46,000 birds on the Nigerian farm have been killed and their bodies disposed of, and Nigerian authorities have banned the movement of birds and people from the farm. Officials also are investigating whether birds were transferred to other farms in the past 21 days, and they, too, are being quarantined, he said. Health officials had feared a deadly bird flu virus could enter impoverished, loosely governed African regions, where many people raise chickens at home for personal consumption.
Source: http://www.cbsnews.com/stories/2006/02/08/ap/health/mainD8FL0PNG5.shtml

27. *February 08, Agence France−Presse* — **Hunt for northern Iraq's poultry moves to the city.** The hunt for poultry to head off a possible avian flu epidemic in Iraq's northern Kurdish provinces has moved down from the remote mountains into the environs of Sulaimaniyah amid news of a second death from the virus. "Since the beginning of February, we started a campaign of exterminating domestic birds to protect Sulaimaniyah," said Sirwan Mohammed Saleh, an agricultural engineer working with a team in the village of Awal, just to the southwest of the

city. The valley of Sulaimaniyah has long been popular with migratory birds. Afraid that this wave of itinerant visitors might pass the virus onto to their domestic cousins living in the valley, all birds within a nine mile radius of the city are being culled. Until last week, only the mountainous region of Raniya, 112 miles to the north of the city and where most of the suspected cases had been found, was the focus of the culling teams. Now the birds of the provincial capital are being targeted as well. In the village of Awal, the veterinary teams are busy playing cat and mouse games with the villagers. Forewarned of the search, some have hidden their chickens or released them, while others hurriedly ate them.
Source: http://news.yahoo.com/s/afp/20060208/wl_mideast_afp/healthfluiraqhunt_060207163905;_ylt=Am2Dxtjqr64h2klmE2k5OP2JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

28. *February 08, Reuters* — **China reports bird flu outbreak, new human case.** China reported a fresh outbreak of bird flu on a chicken farm in the northern province of Shanxi on Wednesday, February 8, and also said another person was being treated for the virus in the east of the country. The latest bird flu patient brought the number of the country's confirmed cases in humans to 11. Seven people are known to have died from the virus in China. The victim, a 26−year−old woman from eastern China's Fujian province, was in a stable condition. China said the outbreak in poultry in the north was now under control. By Friday, 15,000 chickens in Yijing township, part of the city of Yangquan, had died, the Ministry of Health said in a report on its Website. They were confirmed to have the H5N1 strain of avian flu on Tuesday, February 7. Teams from the Agriculture Ministry had been sent to Yijing, where more than 187,000 chickens were culled, and the outbreak was brought under control, it said. Veterinarian departments had not detected any bird flu outbreak in animals in the area where the sick woman lives. With more poultry than anywhere else in the world, China is seen as a key battleground in fighting the disease.
Source: http://abcnews.go.com/US/wireStory?id=1594206

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

29. *February 07, Reporter (CA)* — **Health and emergency officials say California county isn't ready for flu pandemic.** In the wake of a recent drill, Solano County, CA's, public health and emergency officials believe local agencies have more to do if they are going to be prepared for an avian flu pandemic. The drill found a number of issues needing further work, said Robin Cox, county health education manager. Among the issues was the need for greater language capabilities so that the emergency situation could be clearly communicated to Solano's diverse population. Also identified was the need to forge closer working relationships with surgery centers, skilled nursing facilities and other clinics that have access to medical equipment and supplies; strengthening the county's mass casualty plans; identifying and reaching special and

sometimes hard−to−reach populations such as people who are homeless, vision impaired, hearing impaired, elderly, needing special assistance with medical equipment such as oxygen; dealing with the aftermath of mental health and psychological issues and making sure businesses and Chambers of Commerce are involved in planning efforts.
Source: http://thereporter.com/news/ci_3484144

30. *February 07, Miami Herald (FL)* — **Florida kicks off campaign on disaster preparedness.** Florida Governor Jeb Bush announced a new disaster−readiness campaign Monday, February 6, after completing an exercise to test the state's response to a terrorist−made flu pandemic. Bush said the campaign, on the Web at mysafeflorida.org, will complement his proposed "Culture of Preparedness" effort to help private citizens and government better cope with disasters. The governor gave out little information about the results of the round−table flu−pandemic exercise. However, Bush said the state has a good record of responding quickly to disasters. "The good news is that when you prepare for one disaster −− whether it's man−made or natural −− you're really preparing for all of them," he said. "If there is a flu pandemic I promise you there'll be a very aggressive communications strategy." The governor's public−awareness campaign was launched Monday with seven press conferences throughout the state.
Disaster−readiness campaign: http://www.mysafeflorida.org/
Source: http://www.miami.com/mld/miamiherald/news/local/states/florida/counties/broward_county/13808333.htm

31. *February 07, CBS 11 News (TX)* — **Officials say Dallas homeland security lacking.** Nearly four and a half years after the 9/11 terror attacks, Dallas County, TX, commissioners say the county's homeland security is still inadequate. Dallas County Commissioners gave two weeks to their new Homeland Security Chief to come up with a list of needs. Furthermore, the county lacked a Homeland Security Director for more than six months. If Dallas County was hit by terrorists or faced multiple wildfires it would have a tough time coordinating its response. While the county has an emergency response center with computers, there are no employees to use them. And the county's new director of security and emergency management acknowledges the room doesn't have a back−up generator. At Dallas County Commissioners' Court Tuesday, February 7, Judge Margaret Keliher called for a new plan to bring the county up to standards in two weeks.
Source: http://cbs11tv.com/topstories/local_story_038230235.html

[Return to top]

Information Technology and Telecommunications Sector

32. *February 08, Zone−H* — **High−risk vulnerability in Lexmark Printer Sharing service.** There is a high−risk vulnerability in the Lexmark Printer Sharing service which could allow a remote, unauthenticated attacker to execute arbitrary code on a Lexmark printer user's computer system with Local System privileges. There is no known official patch or workaround for this issue.
Source: http://www.zone−h.org/en/advisories/read/id=8680/

33. *February 08, VNUNet* — **Windows hit by yet another WMF hole.** Microsoft has issued a

warning about a new vulnerability in the Windows Meta File (WMF) image format that affects older versions of Internet Explorer (IE). The vulnerability exists in IE 5.5 running on Windows 2000 and IE 5.01 on Windows ME. Users of IE 6 or other Windows versions are not affected by this vulnerability, Microsoft emphasized in a security advisory.
Microsoft Security Advisory: http://www.microsoft.com/technet/security/advisory/913333.mspx
Source: http://www.vnunet.com/vnunet/news/2149931/windows−hit−yet−wm f−hole

34. *February 07, FrSIRT* — **IBM Lotus Domino LDAP server remote denial−of−service vulnerability.** A vulnerability has been identified in IBM Lotus Domino, which could be exploited by remote attackers to cause a denial of service. This flaw is due to an error in the LDAP service that fails to properly handle malformed requests sent to port 389/TCP, which could be exploited by remote attackers to cause a denial of service by sending a specially crafted LDAP request to a vulnerable system. Solution: The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2006/0458

35. *February 07, Tech Web* — **Islamic messages deface hundreds of Danish sites.** Muslim protests over editorial cartoons originally published by a Danish newspaper have spilled onto the Internet and resulted in defacements of nearly 600 Danish Websites with anti−Dane, pro−Muslim messages in the past week, Helsinki−based F−Secure said Tuesday, February 7. This has been the latest fallout in the uproar over cartoons that include one depicting Mohammed with a bomb for a turban. The defacements included warnings of suicide bombings, Arabic−language messages sprawled across home pages, and threats such as "die plez."
Source: http://www.securitypipeline.com/news/179101482

36. *February 07, Tech Web* — **Microsoft says Kama Sutra worm overblown.** As users and security firms reported little damage done by the Kama Sutra worm, a manager of Microsoft's anti−virus development team warned that overhyping threats could lead to a "cry wolf" syndrome where future alerts aren't taken seriously. "Too much hype in situations that end in false alarms ends up diluting the meaning of warnings for true worldwide threats," wrote Matt Braverman, a program manager with Microsoft's anti−malware team, on the group's blog. In particular, Braverman criticized those who called out warnings based on a Web counter that, though initially reporting the number of Kama Sutra infections accurately, was manipulated later in the process to claim millions of machines had been compromised. Braverman's comments were in sync with earlier positions taken by Microsoft in January on the worm.
Source: http://www.securitypipeline.com/news/179101481

37. *February 07, IDG News* — **Attack code published for Firefox flaw.** A hacker Tuesday, February 7, published code that exploits a vulnerability found in the latest version of Mozilla Corp.'s Firefox browser. The code, which targets the Firefox 1.5 browser, was posted Tuesday on The Metasploit Project site by a hacker known as H D Moore. Metasploit is a widely used hacking tool. Moore said that a hacker by the name of Georgi Guninski reported the flaw to the Mozilla Foundation on December 6, and that he had simply implemented and posted the technique described by Guninski. Mozilla published an advisory about the exploit last Wednesday as it released the Firefox 1.5.0.1 browser, which included a patch for the flaw.

According to the advisory, the vulnerability, which had been rated as moderate, causes a corruption in the browser's memory that could be exploitable to run arbitrary code. Hacker Aviv Raff on Tuesday criticized Mozilla in his blog for under−rating the flaw. He has blasted the open−source group in the past for downplaying the seriousness of vulnerabilities that have been found in its software.
Source: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,108469,00.html?SKC=security−108469

38. *February 07, I.T. Vibe* — **Spanish hacker sentenced to two years in jail and fine of $1.6 million.** Experts at Sophos have welcomed the news that a hacker who stopped over a third of Spanish computer users from using the Internet has been sentenced to two years in jail. Santiago Garrido, 26, used a computer worm to launch Distributed Denial−of−Service (DDoS) attacks after he was expelled from the popular "Hispano" IRC chat room for not following rules. The attacks disrupted an estimated three million users of the Wanadoo, ONO, Lleida Net and other Internet service providers, amounting to a third of all of Spain's Internet users at the time of the offence in 2003. Garrido, who went by the aliases "Ronnie" and "Mike25", was sentenced at a court in La Coruña and also faces a $1.6 million fine.
Source: http://itvibe.com/news/3912/

39. *February 06, Security Focus* — **Study: Spyware remains rampant as Winamp exploited.** A new study by the University of Washington finds that one in twenty executables on the Internet contain spyware. The study, which sampled more than 20 million Internet addresses, also found other disturbing trends. Among them: one in 62 Internet domains contains "drive−by download attacks," which try to force spyware onto the user's computer simply by visiting the Website. The problems for Web surfers primarily affect Microsoft's Internet Explorer browser but exist to a lesser extent for other browsers as well.
University of Washington study:
http://www.cs.washington.edu/homes/gribble/papers/spycrawler .pdf
Source: http://www.securityfocus.com/brief/128

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of several vulnerabilities in Mozilla. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary JavaScript commands with elevated privileges or cause a denial of service condition on a vulnerable system.

For more information please review US−CERT Vulnerability Note:

VU#592425

Mozilla based browsers fail to validate user input to the attribute name in "XULDocument.persist" at URL:

http://www.kb.cert.org/vuls/id/592425

US−CERT urges users and administrators to implement the following recommendations.

Review updates to:

Firefox 1.5.0.1: http://www.mozilla.com/firefox/

SeaMonkey 1.0: http://www.mozilla.org/projects/seamonkey/

Disable JavaScript in Thunderbird and Mozilla Suite.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4556 (−−−), 6881 (bittorrent), 445 (microsoft−ds), 26777 (−−−), 25 (smtp), 139 (netbios−ssn), 135 (epmap), 1025 (win−rpc), 40000 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

40. *February 08, VoiceNews (MI)* — **Nerve center for Super Bowl security.** Buried deep inside a brick building not far from the runway at Selfridge Air National Guard Base, located 22 miles east of Warren, MI, is the Joint Air Special Operation Center, the nerve center that kept airspace over Detroit safe and secure last weekend during the Super Bowl. Inside, representatives from many agencies including the Federal Bureau of Investigation, Michigan State Police, Detroit Police Department, U.S. Air Marshal Service, U.S. Coast Guard, Air National Guard, Canadian Air Force, and NORAD worked away at the task of keeping the NFL's first international Super Bowl safe from any terrorist threat. Commanding the entire Super Bowl security effort was Rear Adm. Robert J. Papp, Commander of the U.S. Coast Guard Ninth District and tapped by Department of Homeland Security Secretary Michael Chertoff to head the effort. “We're always a busy border area, midway between the Blue Water Bridge in Port Huron and the tunnel and bridge crossings in Detroit,” Papp said. To address technical and jurisdictional problems the indefinite border running down the center of the Detroit River, Lake St. Clair, and the St. Clair River presents, the U.S. Coast Guard deputized several members of the Royal Canadian Mounted Police.
Source: http://www.voicenews.com/stories/020806/loc_selfridge001.sht ml

41.

February 08, Reuters — **NATO to patrol no−fly ban at Games start.** Italy will close the airspace over Turin and NATO will patrol the skies on Friday, February 10, when athletes and foreign dignitaries including Laura Bush, the U.S. first lady, attend the Winter Olympics opening ceremony. The no−fly order was the latest move to protect the thousands of athletes and at least 15 visiting foreign leaders gathering in Turin for the Games, which start with the opening ceremony at 8 p.m. (1900 GMT) on Friday. Wary of both terrorist threats and anti−globalization protesters, Italy has deployed thousands of police, snipers and armed skiers to patrol the slopes, venues and living quarters of athletes staying in Turin and villages in the nearby Alps. In addition to some 9,000 police, Italy will deploy 1,350 skiers from its special Alpine force to patrol and groom the slopes during the Games, as well as 400 parachutists. NATO will send two E−3D surveillance aircraft to patrol the skies during the Games, the alliance said on Wednesday, February 8. Security officials say they have had no specific terrorist threats against Turin in contrast to security concerns that dogged the Athens Games in 2004.
Source: http://abcnews.go.com/International/wireStory?id=1594224

42. *February 08, Associated Press* — **Dark SUV sought in Alabama church fire investigation.** Federal agents said Wednesday, February 8, they were looking for a dark sport utility vehicle (SUV) in the investigation of nine rural Alabama church fires. Two members of Old Union Baptist Church in Bibb County said they saw just such a vehicle driving slowly by the church at Brierfield when they arrived moments after the fire was set around 4:05 a.m. CST Friday, February 3. All five fires have been ruled arsons, and federal agents say they are working on the assumption that the four Tuesday, February 7, in west Alabama are linked to those in Bibb County. Witnesses and authorities reported a similar pattern at several of the burned churches, including Old Union −− a door kicked in and the fire set near the pulpit. Witnesses in west Alabama also reported seeing a dark SUV near at least one of the burned churches. The four churches that burned Tuesday in three adjoining counties on the Mississippi line all have black congregations. But four of the five churches set afire in Bibb County have white congregations. Agents said they do not have a motive in the arsons.
Source: http://www.cbsnews.com/stories/2006/02/08/ap/national/mainD8 FL3Q787.shtml

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.